



# FortiOS - Release Notes

VERSION 5.2.8

**FORTINET DOCUMENT LIBRARY**

<http://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<http://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTIGATE COOKBOOK**

<http://cookbook.fortinet.com>

**FORTINET TRAINING SERVICES**

<http://www.fortinet.com/training>

**FORTIGUARD CENTER**

<http://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<http://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdocs@fortinet.com](mailto:techdocs@fortinet.com)



March 22, 2017

FortiOS 5.2.8 Release Notes

01-528-377753-20170322

# TABLE OF CONTENTS

Change Log .....	5
<b>Introduction .....</b>	<b>6</b>
Supported models .....	6
Last Release of Software .....	7
<b>Special Notices .....</b>	<b>8</b>
Compatibility with FortiOS versions .....	8
Removed WANOPT, NETSCAN, FEXP features from USB-A .....	8
Removed Local Report Customization .....	8
Router Prefix Sanity Check .....	9
WAN Optimization in FortiOS 5.2.4 .....	9
Built-In Certificate .....	9
FortiGate-92D High Availability in Interface Mode .....	9
Default log setting change .....	9
FG-5001D operating in FortiController or Dual FortiController mode .....	9
FortiGate units running 5.2.8 .....	10
Firewall services .....	10
FortiPresence .....	10
SSL VPN setting page .....	10
<b>Upgrade Information .....</b>	<b>11</b>
Upgrading from FortiOS 5.2.6 or later .....	11
Upgrading from FortiOS 5.0.12 or later .....	11
Downgrading to previous firmware versions .....	11
FortiGate VM firmware .....	11
Firmware image checksums .....	12
<b>Product Integration and Support .....</b>	<b>13</b>
FortiOS 5.2.8 support .....	13
Language support .....	15
SSL VPN support .....	16
SSL VPN standalone client .....	16
SSL VPN web mode .....	16
SSL VPN host compatibility list .....	17
<b>Resolved Issues .....</b>	<b>18</b>
<b>Known Issues .....</b>	<b>24</b>

**Limitations ..... 28**

    Citrix XenServer limitations .....28

    Open Source XenServer limitations ..... 28

## Change Log

Date	Change Description
2016-06-29	Initial release.
2016-06-30	Added 377928 to Known Issues. Added 245986 and 375341 to Resolved Issues.
2016-07-04	Updated SSL VPN information.
2016-07-08	Updated Upgrade <i>Information</i> > <i>Upgrade Paths URL</i> . Added 369353 to Resolved Issues.
2016-07-13	Added 274252 to Resolved Issues.
2016-07-25	Added 370337 to Resolved Issues.
2016-08-15	Updated Supported Models, FG-5001B, C, D, and 5101C released on build 9143.
2016-08-17	Added 377753 to Known Issues.
2016-08-30	Added 385860 to <i>Known Issues</i> > <i>FortiGate-3815D</i> .
2016-09-01	Added 374283 to <i>Known Issues</i> > <i>Webfilter</i> .
2016-09-14	Added <i>Special Notices</i> > <i>Removed Local Report Customization</i> section.
2016-09-21	Added 388032 to <i>Known Issues</i> > <i>System</i> .
2017-03-22	Removed 273910 from <i>Known Issues</i> .

# Introduction

This document provides the following information for FortiOS 5.2.8 build 0727:

- [Special Notices](#)
- [Upgrade Information](#)
- [Product Integration and Support](#)
- [Resolved Issues](#)
- [Known Issues](#)
- [Limitations](#)

See the [Fortinet Document Library](#) for FortiOS documentation.

## Supported models

FortiOS 5.2.8 supports the following models.

<b>FortiGate</b>	FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-SFP, FG-60C-POE, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FGT-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-310B-DC, FG-311B, FG-400D, FG-500D, FG-620B, FG-620B-DC, FG-621B, FG-600C, FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-1500DT, FG-3000D, FG-3100D, FG-3040B, FG-3140B, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3810D, FG-3815D, FG-3950B, FG-3951B
<b>FortiWiFi</b>	FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-3G4G-VZW, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D
<b>FortiGate Rugged</b>	FGR-60D, FGR-100C
<b>FortiGate VM</b>	FG-VM64, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN
<b>FortiSwitch</b>	FS-5203B
<b>FortiOS Carrier</b>	FCR-3950B and FCR-5001B FortiOS Carrier 5.2.8 images are delivered upon request and are not available on the customer support firmware download page.  FortiOS Carrier firmware image file names begin with <i>FK</i> .

The following models are released on a special branch based off of FortiOS 5.2.8. As such, the *System > Dashboard > Status* page and the output from the `get system status` CLI command displays the build number.



**FGT-VM64-AWS/AWSONDEMAND**

Released on build 9141.

**FGT-VM64-AZURE**

Released on build 5464.

**FG-5001B**

Released on build 9143.

**FG-5001C**

Released on build 9143.

**FG-5001D**

Released on build 9143.

**FG-5101C**

Released on build 9143.

To confirm that you are running the proper build, the output from the `get system status` CLI command has a **branch point field** that should read 0727.



The FG-60D-3G4G-VZW model uses the FGT\_60D\_MC-v5-build0727-FORTINET.out image. The FWF-60D-3G4G-VZW model uses the FWF\_60D\_MC-v5-build0727-FORTINET.out image.

## Last Release of Software

Due to the device flash size limitations, the following FortiGate models' last release of software will be FortiOS version 5.2.5. It is noted that these devices already have entered into their End-of-Life Cycle. Further details and exact dates can be found on the [Fortinet Customer Support portal](#):

### Affected Products:

- FortiGate FG-3016B
- FortiGate FG-3810A
- FortiGate FG-5001A SW & DW
- FortiCarrier FK-3810A
- FortiCarrier FK-5001A SW & DW

# Special Notices

## Compatibility with FortiOS versions

The following units have a new WiFi module built-in that is not compatible with FortiOS 5.2.1 and lower. It is recommended to use FortiOS 5.2.2 and later for these units.

### Affected models

Model	Part Number
FWF-60CX-ADSL	PN: 8918-04 and later

The following units have a memory compatibility issue with FortiOS 5.2.1 and lower. It is recommended to use FortiOS 5.2.2 and later for these units.

### Affected models

Model	Part Number
FG-600C	PN: 8908-08 and later
FG-600C-DC	PN: 10743-08 and later
FG-600C-LENC	PN: 11317-07 and later

## Removed WANOPT, NETSCAN, FEXP features from USB-A

The following features have been removed from the FortiGate and FortiWiFi 80C, 80CM, and 81CM:

- WAN Optimization
- Vulnerability scanning
- Using FortiExplorer on a smartphone to manage the device by connecting to the USB-A port

## Removed Local Report Customization

Local report customization has been removed from FortiOS v5.2. You can still record and view local reports, but you can no longer customize their appearance. For more control over customizing local reports, you can use FortiAnalyzer or FortiCloud.



## Router Prefix Sanity Check

Prior to FortiOS 5.2.4 under the config router prefix table, if there are any `le` and `ge` settings that have the same prefix length as the prefix, you may lose the prefix rule after upgrading to FortiOS 5.2.4 or later.

## WAN Optimization in FortiOS 5.2.4

In FortiOS 5.2.4:

- If your FortiGate does not have a hard disk, WAN Optimization is not available.
- If your FortiGate has a hard disk, you can configure WAN Optimization from the CLI.
- If your FortiGate has two hard disks, you can configure WAN Optimization from the GUI.

See the [FortiOS 5.2.4 Feature Platform Matrix](#) to check the availability for your FortiGate model.

## Built-In Certificate

FortiGate and FortiWiFi D-series and above have a built in Fortinet\_Factory certificate that uses a 2048-bit certificate with the 14 DH group.

## FortiGate-92D High Availability in Interface Mode

The FortiGate-92D may fail to form an HA cluster and experience a spanning tree loop if it is configured with the following:

- operating in interface mode
- at least one of the interfaces, for example *interface9*, is used as the HA heartbeat interface
- a second interface is connected to an external switch

Workaround: use either WAN1 or WAN2 as the HA heartbeat device.

## Default log setting change

For FG-5000 blades and FG-3900 series, log disk is disabled by default. It can only be enabled via CLI. For all 2U & 3U models (FG-3600/FG-3700/FG-3800), log disk is also disabled by default. For all 1U models and desktop models that supports SATA disk, log disk is enabled by default.

## FG-5001D operating in FortiController or Dual FortiController mode

When upgrading a FG-5001D operating in FortiController or dual FortiController mode from version 5.0.7 (B4625) to FortiOS version 5.2.3, you may experience a back-plane interface connection issue. This is due to a change to

the ELBC interface mapping ID. After the upgrade, you will need to perform a factory reset and then re-configure the device.

## FortiGate units running 5.2.8

FortiGate units running 5.2.8 and managed by FortiManager 5.0.0 or 5.2.0 may report installation failures on newly created VDOMs, or after a factory reset of the FortiGate unit even after a retrieve and re-import policy.

For the latest information, see the [FortiManager and FortiOS Compatibility](#).

## Firewall services

Downgrading from 5.2.3 to 5.2.2 may cause the default protocol number in the firewall services to change. Double check your configuration after downgrading to 5.2.2.

## FortiPresence

For FortiPresence users, it is recommended to change the FortiGate web administration TLS version in order to allow the connection.

```
config system global
    set admin-https-ssl-versions tlsv1-0 tlsv1-1 tlsv1-2
end
```

## SSL VPN setting page

The default server certificate has been changed to the `Fortinet_Factory` option. This excludes FortiGate-VMs which remain at the `self-signed` option. For details on importing a CA signed certificate, please see the [How to purchase and import a signed SSL certificate](#) document.

# Upgrade Information

## Upgrading from FortiOS 5.2.6 or later

FortiOS version 5.2.8 officially supports upgrade from version 5.2.6 or later.

## Upgrading from FortiOS 5.0.12 or later

FortiOS version 5.2.8 officially supports upgrade from version 5.0.12 or later.



When upgrading from a firmware version beyond those mentioned in the Release Notes, a recommended guide for navigating the upgrade path can be found on the Fortinet documentation site.

There is separate version of the guide describing the safest upgrade path to the latest patch of each of the supported versions of the firmware. To upgrade to this build, go to [FortiOS 5.2 Supported Upgrade Paths](#)

## Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- VDOM parameters/settings
- admin user account
- session helpers
- system access profiles.

## FortiGate VM firmware

Fortinet provides FortiGate VM firmware images for the following virtual environments:

### Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the QCOW2 file for Open Source XenServer.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

### Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains QCOW2 that can be used by `qemu`.

### Microsoft Hyper-V

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.hyperv.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains three folders that can be imported by Hyper-V Manager on Hyper-V 2012. It also contains the file `fortios.vhd` in the Virtual Hard Disks folder that can be manually added to the Hyper-V Manager.

### VMware ESX and ESXi

- `.out`: Download either the 32-bit or 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.ovf.zip`: Download either the 32-bit or 64-bit package for a new FortiGate VM installation. This package contains Open Virtualization Format (OVF) files for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

## Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, <https://support.fortinet.com>. After logging in select *Download > Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

# Product Integration and Support

## FortiOS 5.2.8 support

The following table lists 5.2.8 product integration and support information:

<b>Web Browsers</b>	<ul style="list-style-type: none"><li>• Microsoft Internet Explorer version 11</li><li>• Mozilla Firefox version 42</li><li>• Google Chrome version 46</li><li>• Apple Safari version 7.0 (For Mac OS X)</li></ul> <p>Other web browsers may function correctly, but are not supported by Fortinet.</p>
<b>Explicit Web Proxy Browser</b>	<ul style="list-style-type: none"><li>• Microsoft Internet Explorer versions 8, 9, 10, and 11</li><li>• Mozilla Firefox version 27</li><li>• Apple Safari version 6.0 (For Mac OS X)</li><li>• Google Chrome version 34</li></ul> <p>Other web browsers may function correctly, but are not supported by Fortinet.</p>
<b>FortiManager</b>	<p>For the latest information, see the <a href="#">FortiManager and FortiOS Compatibility</a>.</p> <p>You should upgrade your FortiManager prior to upgrading the FortiGate.</p>
<b>FortiAnalyzer</b>	<p>For the latest information, see the <a href="#">FortiAnalyzer and FortiOS Compatibility</a>.</p> <p>You should upgrade your FortiAnalyzer prior to upgrading the FortiGate.</p>
<b>FortiClient Microsoft Windows and FortiClient Mac OS X</b>	<ul style="list-style-type: none"><li>• 5.4.0 and later</li><li>• 5.2.5 and later</li></ul>
<b>FortiClient iOS</b>	<ul style="list-style-type: none"><li>• 5.4.1</li><li>• 5.2.2 and later</li></ul>
<b>FortiClient Android and FortiClient VPN Android</b>	<ul style="list-style-type: none"><li>• 5.2.8</li><li>• 5.2.7</li></ul>

**FortiAP**

- 5.2.5 and later
- 5.0.10

You should verify what the current recommended FortiAP version is for your FortiAP prior to upgrading the FortiAP units. You can do this by going to the *WiFi Controller > Managed Access Points > Managed FortiAP* page in the GUI. Under the *OS Version* column you will see a message reading *A recommended update is available* for any FortiAP that is running an earlier version than what is recommended.

**FortiSwitch OS (FortiLink support)**

- 3.4.2 build 0192 and later
- Supported models: all FortiSwitch D models.

**FortiSwitch-ATCA**

- 5.0.3 and later
- Supported models: FS-5003A, FS-5003B

**FortiController**

- 5.2.0 and later
- Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C
- 5.0.3 and later
- Supported model: FCTL-5103B

**FortiSandbox**

- 2.2.1
- 2.1.0

**Fortinet Single Sign-On (FSSO)**

- 5.0 build 0250 (needed for FSSO agent support OU in group filters)
  - Windows Server 2008 (64-bit)
  - Windows Server 2008 R2 64-bit
  - Windows Server 2012 Standard
  - Windows Server 2012 R2 Standard
  - Novell eDirectory 8.8
- 4.3 build 0164 (contact [Support](#) for download)
  - Windows Server 2003 R2 (32-bit and 64-bit)
  - Windows Server 2008 (32-bit and 64-bit)
  - Windows Server 2008 R2 64-bit
  - Windows Server 2012 Standard Edition
  - Windows Server 2012 R2
  - Novell eDirectory 8.8

FSSO does not currently support IPv6.

**FortiExplorer**

- 2.6 build 1083 and later.

Some FortiGate models may be supported on specific FortiExplorer versions.

**FortiExplorer iOS**

- 1.0.6 build 0130 and later

Some FortiGate models may be supported on specific FortiExplorer iOS versions.

<b>FortiExtender</b>	<ul style="list-style-type: none"> <li>• 3.0.0 build 0069</li> <li>• 2.0.0 build 0003 and later</li> </ul>
<b>AV Engine</b>	<ul style="list-style-type: none"> <li>• 5.177</li> </ul>
<b>IPS Engine</b>	<ul style="list-style-type: none"> <li>• 3.169</li> </ul>
<b>Virtualization Environments</b>	
<b>Citrix</b>	<ul style="list-style-type: none"> <li>• XenServer version 5.6 Service Pack 2</li> <li>• XenServer version 6.0 and later</li> </ul>
<b>Linux KVM</b>	<ul style="list-style-type: none"> <li>• RHEL 7.1/Ubuntu 12.04 and later</li> <li>• CentOS 6.4 (qemu 0.12.1) and later</li> </ul>
<b>Microsoft</b>	<ul style="list-style-type: none"> <li>• Hyper-V Server 2008 R2, 2012, and 2012 R2</li> </ul>
<b>Open Source</b>	<ul style="list-style-type: none"> <li>• XenServer version 3.4.3</li> <li>• XenServer version 4.1 and later</li> </ul>
<b>VMware</b>	<ul style="list-style-type: none"> <li>• ESX versions 4.0 and 4.1</li> <li>• ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5 and 6.0</li> </ul>

## Language support

The following table lists language support information.

### Language support

Language	GUI
English	✓
Chinese (Simplified)	✓
Chinese (Traditional)	✓
French	✓
Japanese	✓
Korean	✓
Portuguese (Brazil)	✓
Spanish (Spain)	✓

## SSL VPN support

### SSL VPN standalone client

The following table lists SSL VPN tunnel client standalone installer for the following operating systems.

#### Operating system and installers

Operating System	Installer
Microsoft Windows XP SP3 (32-bit) Microsoft Windows 7 (32-bit & 64-bit) Microsoft Windows 8 (32-bit & 64-bit) Microsoft Windows 8.1 (32-bit & 64-bit)	2328
Microsoft Windows 10 (32 bit & 64 bit)	2329
Linux CentOS 6.5 (32-bit & 64-bit) Linux Ubuntu 12.0.4 (32-bit & 64-bit)	2328
Virtual Desktop for Microsoft Windows 7 SP1 (32-bit)	2328

Other operating systems may function correctly, but are not supported by Fortinet.

### SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

#### Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit)	Microsoft Internet Explorer versions 9, 10 and 11 Mozilla Firefox version 33
Microsoft Windows 7 SP1 (64-bit)	Microsoft Internet Explorer versions 9, 10, and 11 Mozilla Firefox version 33
Microsoft Windows 8/8.1 (32bit/62bit)	Microsoft Internet Explorer versions 10 and 11 Mozilla Firefox 42
Mac OS 10.9	Safari 7
Linux CentOS version 5.6	Mozilla Firefox version 5.6
Linux Ubuntu version 12.0.4	Mozilla Firefox version 5.6



Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

## SSL VPN host compatibility list

The following table lists the antivirus and firewall client software packages that are supported.

### Supported Microsoft Windows XP antivirus and firewall software

Product	Antivirus	Firewall
Symantec Endpoint Protection 11	✓	✓
Kaspersky Antivirus 2009	✓	
McAfee Security Center 8.1	✓	✓
Trend Micro Internet Security Pro	✓	✓
F-Secure Internet Security 2009	✓	✓

### Supported Microsoft Windows 7 32-bit antivirus and firewall software

Product	Antivirus	Firewall
CA Internet Security Suite Plus Software	✓	✓
AVG Internet Security 2011		
F-Secure Internet Security 2011	✓	✓
Kaspersky Internet Security 2011	✓	✓
McAfee Internet Security 2011	✓	✓
Norton 360™ Version 4.0	✓	✓
Norton™ Internet Security 2011	✓	✓
Panda Internet Security 2011	✓	✓
Sophos Security Suite	✓	✓
Trend Micro Titanium Internet Security	✓	✓
ZoneAlarm Security Suite	✓	✓
Symantec Endpoint Protection Small Business Edition 12.0	✓	✓

# Resolved Issues

The following issues have been fixed in version 5.2.8. For inquiries about a particular bug, please contact [Customer Service & Support](#).

## DLP

Bug ID	Description
369307	Specific files are detected by DLP even when AV is enabled.
365320	DLP incorrectly matches cookie called <i>name</i> as a filename.
277594	Proxyworker stop working (watchdog timeout) when using IMAPS or when POP3 receives email blocked by DLP.

## Firewall

Bug ID	Description
294760	SNAT issue with IPPPOOL fixed-port-range and static VIP.
369659	Incorrect <code>Seq#</code> translation.
368191	B646- Session Helper is not translating FTP PORT when FTP Active is used.
369353	MAC address are intermittently updated in NPU offload IPv4 sessions.

## FOC

Bug ID	Description
371387	Upgrading from 5.0.11 to 5.2.7 returns an <i>Image RSA signature is invalid</i> error.

## GUI

Bug ID	Description
277780	GUI temporarily unavailable.
271495	<code>pyfcgid</code> uses 99% CPU usage causes Managed FAP GUI stops responding.
290648	Managed AP page does not load.
307770	Network interface is not displayed in VDOMs. Child interface error.

Bug ID	Description
288896	Fetch Base DN interoperability issue with Oracle ODSEE 11.1 LDAP.
363323	FGT-70D/60D GUI for editing Addresses displays error(Internal Server Error).
295912	FAZ is down in Unit Operation widget even though FAZ is connected.

### High Availability

Bug ID	Description
370589	Deny traffic is not logged when HA vclusters are load balanced.
301101	<code>hasync</code> process is running 100% of CPU.
276844	Custom service specifying portrange cannot be synchronized after upgrade.
270267	<i>DUAL Chassis - Standby Chassis Firewall</i> sends traffic.
286827	BGP MD5 authentication error after HA failover.
365669	FGSP can not establish session-helper protocols in asymmetrical traffic environment (e.g. ftp passive-mode) (TP-mode).
281112	HA(A-A) Running FIPS mode 5.0.12 stops reporting.
309532	Not all of IPsec SAs are synced after rebooting slave box.
366745	FortiCloud can not be activated via HA GUI with 2 brand new boxes.
357298	FGSP HA: after policy installation, session hardware off-load partially works.
283697	When a new device joins, the list of devices does not sync between master and slave.

### IPS

Bug ID	Description
301117	IPS consumes 99.9% even with very low traffic. IPS engine version 3.153.

### IPSec

Bug ID	Description
367414	Packets dropped when IPSec is configured with algorithm unsupported on NP4.

Bug ID	Description
365288	IPsec <code>phase1</code> in zones with both <code>src</code> and <code>dst</code> interfaces, the zone tunnel policy shown as <code>NONE</code> .
287382	Username disappears from IKEv2 tunnel in IPsec monitor after rekey.
309458	Pass through NAT-T IPsec traffic can not be offloaded by NP6
274252	IPsec VPN <code>phase1</code> interface does not negotiate SA with its peer when 3G interface comes up.

## Logging

Bug ID	Description
373083	Broken remote log capabilities when <code>resolve-ip</code> is enabled.
301401	Local Report is generated even if it is disabled.
368496	One time schedule pre-expiration event log not generated in multi-vdom environments.

## Routing

Bug ID	Description
364309	Resolved IP is listed as <code>MISSING</code> and no route created.
265712	<code>pdmd</code> (pim dense mode) signal 11 crash.
309721	Backup FG sends VRRP advertisement on I/F link up.
298214	If two of four GWs for policy routes go down, one <code>proute</code> down but another <code>proute</code> incorrectly up
357487	<code>pim-sm bsr</code> flooding heavily on FGT

## SSL VPN

Bug ID	Description
364918	<code>SSLVPN_TUNNEL_ADDR1</code> added to TP mode vdom when system reboots.
276730	When split-tunneling is set to a non default value, it is not shown in the config.
371276	SSL client can not login proxy smb/cifs server.
290818	SSL VPN stops working when canceling a SSL VPN webmode ftp upload.

Bug ID	Description
306982	Auth policy is ignored if the specified user is a member of group in the following policy.

## System

Bug ID	Description
282204	NP6 Anomaly settings not working.
372632	FGT-3700D kernel crash.
373033	Deep SSL inspection stops working when <i>Inspect All Ports</i> is enabled.
371660	FMG fails to set <code>uninterruptible-upgrade</code> settings.
365497	Possible packet out-of-order with NP6 during established TCP session.
367471	Fragmented out-of-sequence ICMP Reply can loop endlessly in npu-vlink.
356245	FortiGate is ignores remote side change Aggregation IDs, and keeping this ports active in LACP.
309821	ICMPv6 packets with <i>Hop-by-Hop Options</i> are not decoded properly by built in sniffer.
374706	Proxyworker memory keep increasing.
355482	LACP negotiation causes wrong HA master election.
356611	Customized portal message cannot be displayed.
304742	IPSec clients need to login twice, except when debug IKE is enabled.
302606	Comlog is disabled by failure to read or <code>Ctrl+C</code> .
368459	No link down trap when a LAG member port is down.
295139	After disabling IPS, UDP traffic from the existing sessions will be blocked.
306321	GRE tunnel interface is mandatory (changed from 5.2.3).
310071	A specific SFP shared port's LED (Port18 on FG-1000C) is not lit properly.
354337	Loss of custom replacement image post upgrade 5.0.X to 5.2.X.
304740	Memory leak in <code>imd</code> .
369526	After restoring VDOM config, the VDOM connectivity is completely lost.
309844	Packets dropped by nturbo sometimes causing unclosed sessions.

Bug ID	Description
302908	<code>smbcd</code> continuously requests for memory and causes system to go into conserve mode.
307191	Upload speed reduced and system CPU increased when IPsec is offloaded to SP2.
310195	Sometimes LACP failed to negotiate on FG-100D.
245986	SNMP clients blocks trap requests to SNMP server

## User

Bug ID	Description
293299	2FA email token expiration issues for LDAP users.
307920	<code>authd</code> inserted two non-portrange entries into FSSO list with the same IP address.

## WANopt & Webproxy

Bug ID	Description
365345	Application <code>WAD</code> signal 11 received.
269979	Web Proxy profile setting is removed in the URL Filter entry when a restricted admin clicks the <i>Apply</i> button in the Web Filter Profile.
309149	Explicit Proxy does not respect assigned outgoing IPs.
375341	<code>WAD</code> stops working at signal 6.

## Web Filter

Bug ID	Description
376338	<i>Blocked Override</i> does not use the assigned profile for certain URLs.
363949	Webfilter overrides does not work when playing videos from Youtube.com.
285017	Safe Search does not work for Yandex.

## WiFi

Bug ID	Description
280395	Client cannot access internet via Captive portal enabled VAP.

**Common Vulnerabilities and Exposures**

Bug ID	Description
370337	FortiOS 5.2.8 is no longer vulnerable to the following CVE References: <ul style="list-style-type: none"><li>• 2016-2107</li><li>• 2016-2105</li><li>• 2016-2106</li><li>• 2016-2109</li><li>• 2016-2176</li></ul> Visit <a href="https://fortiguard.com/psirt">https://fortiguard.com/psirt</a> for more information.

# Known Issues

The following issues have been identified in version 5.2.8. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

## AntiSpam

Bug ID	Description
374283	When there is a matching email address in <code>bwl</code> , exempted traffic may not be included in the AntiSpam log.

## DLP

Bug ID	Description
369825	There may be inconsistent DLP behavior.

## Firewall

Bug ID	Description
375678	<code>update-all-session-timer</code> may not work as expected.

## FortiGate 3810D

Bug ID	Description
285429	Traffic may not be able to go through the NPU VDOM link with traffic shaper enabled on FortiGate-3810D TP mode.

## FortiGate-3815D

Bug ID	Description
385860	FGT-3815D does not support 1GE SFP transceivers.

## FortiGate-VM

Bug ID	Description
272438	During the boot-up sequence, the FortiGate-VM device may encounter a harmless configuration error message.



**FortiSandbox**

Bug ID	Description
269830	The UTM log may incorrectly report a file that has been sent to FortiSandbox. <i>FortiView</i> > <i>FortiSandbox</i> may still show files are submitted even after the daily upload quota has been reached.
273244	On the FortiGate device in <i>FortiView</i> > <i>FortiSandbox</i> , the analysis result may show a pending status and the FortiCloud side may show an unknown status.

**FortiSwitch**

Bug ID	Description
376375	FSW with B0181 (v3.4.1) can be discovered but may not be able to obtain the IP addr and be authorized successfully.

**GUI**

Bug ID	Description
215890	Local-category status display may not change after running <code>unset category-over-ride</code> in the CLI.
246546	Adding an override application signature may cause all category settings to be lost.
267957	The Top Interfering APs chart in the 5G Radio Spectrum Analysis Window may be empty.
268346	<i>All sessions: filter application, threat, and threat type</i> , may not work as expected
271113	When creating an <code>id_based_policy</code> with SSL enabled, and the <code>set gui-multipleutm disable</code> is applied, an <i>Entry not found</i> error message may appear.
278638	Explicit policy may be automatically reset to log security events.
285813	When navigating <i>FortiView</i> > <i>Application</i> some security action filters may not work.
286226	Users may not be able to create new address objects from the Firewall Policy.
310930	LDAP browser in <code>LDAP-group-GUI</code> may not respect group filter from LDAP server.

**HA**

Bug ID	Description
374990	Extended Sequence Number issue in HA firewalls.
368447	FGSP may sync static BFD setting.

## Logging & Report

Bug ID	Description
377928	FortiCloud report may not display on low-end platforms without SSD. <b>Workaround:</b> Upgrade from previous 5.2.6 or 5.2.7 GA release

## System

Bug ID	Description
263864	When the interface is configured with <i>Auto-Speed</i> , FG-3240C NP4 Port 1G may stay down after reboot. <b>Workaround:</b> Set the interface speed to <i>1000/Full</i> .
285520	On NP4 platforms, TCP traffic may not be able to be offloaded in the decryption direction.
285981	Adding more than eight members to LACP <code>get np6_lacp_add_slave</code> may result in an error.
302272	Medium type may be shown incorrectly on shared ports.
375141	When enabled, traffic may appear in the incorrect VDOM but correct VLAN interface.
388032	Corrupted packets may cause malfunction of NP6, which causes NP ports to be unable to accept and forward traffic. <b>Affected models:</b> All NP6 platforms

## VoIP

Bug ID	Description
272278	SIP calls may be denied when using a combination of SIP ALG, IPS, and AppCtrl.

## Webfilter

Bug ID	Description
284661	If the requested URL has port number, the URL filter may not block properly.
377753	Modify antispam logic to handle <code>local-override</code> .

## WiFi

Bug ID	Description
267904	If the client is connecting to an SSID with WPA-Enterprise and User-group, it may not be able to pass the traffic policy.
355335	SSID may stop broadcasting.

# Limitations

## Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

## Open Source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.



**FORTINET®**

High Performance Network Security



Copyright© 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.